TITLE:

A Study on Access Control Mechanism in Storage Devices for Audiovisual Contents(Abstract_要旨)

AUTHOR(S):

Hirai, Tatsuya

CITATION:

Hirai, Tatsuya. A Study on Access Control Mechanism in Storage Devices for Audiovisual Contents. 京都大学, 2016, 博士(情報学)

ISSUE DATE:

2016-07-25

URL:

https://doi.org/10.14989/doctor.r13046

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

（ 続紙 1 ）

京都大学	博士（情報学）	氏名	平井　達哉
論文題目	A Study on Access Control Mechanism in Storage Devices for Audiovisual Contents （記憶装置における動画コンテンツに対するアクセス制御機構に関する研究）		

（論文内容の要旨）

1980年代以降、音楽・動画等の商用コンテンツのデジタル化が進み、これと並行して、様々な大容量の記憶媒体・装置，またそれらを録画・録音及び再生するための機器が多数開発されている。デジタルコンテンツの特徴は、複製が容易であり、また複製時に劣化を生じないということである。このことから、コンテンツの制作者や権利者の許諾を得ないまま、コンテンツが複製され、インターネット上で配布される事態が生じるようになり、テレビ放送局等は、コンテンツの複製可能回数を制限するような仕組みの構築と、その機器への適用を求めるようになった。一方で、PCやサーバ機等の記憶媒体として磁気ディスクを用いたハードディスク装置（HDD）が、多く開発・搭載されてきた。そのビット単価、単体容量、及びランダムアクセス性能は、1990年代後半に光ディスクを上回るようになった。その結果、2000年頃を境に、テレビ番組の録画再生機への搭載が進んだ。しかし、録画を実行したホスト装置以外にHDDを接続した場合は、コンテンツを再生できないようにするための仕組みがホスト装置に組み込まれていた。その主な理由は、HDDがコンピュータシステムの外部記憶装置として開発されてきたために、コンテンツ単位で利用制御を行うための機能が搭載されてこなかったことである。また、近年になって、利用者が放送番組を録画し、それを再生する際に広告（CM）部分を飛ばして本編のみを視聴するといった事態も、機器の普及も相まって増大してきた。このような事態を問題視したテレビ放送局等は、CMを飛ばす視聴形態を禁止することも要請し始めている。

以上のような背景から、学位申請者は、本論文において、HDD等のプロセッサを内蔵する記憶装置を記憶媒体として想定した新しい利用制御機構を提案している。その特徴は、従来の機器にはない新たな機能を記憶装置に搭載することにより、記憶装置自身が中心となって利用制御を達成すること、その結果として機器全体が高い堅牢性を備えるようになること、また不特定のホスト装置で記憶装置に保存されたコンテンツを利用できるようになることである。

本論文は、全8章で構成されている。その概要は以下の通りである。

第1章は序論である。本研究に取り組むに至った社会的な背景及び要請，並びに本研究において目指すべき目標の概要を述べている。

第2章では、まず既存の商用デジタルコンテンツを利用するための機器の構成要素の特定、各構成要素の特性の分析、各構成要素を適用対象として過去に実際に開発された利用制御技術の特性や問題点について述べている。続いて、本研究において考案する利用制御の仕組みが備えるべき基礎特性を規定している。それらは、以下の通りである。(1)動画コンテンツを適切な大きさのブロックに分割し、個々のブロックに、他のブロックの利用実績に依存しない各ブロックに固有の利用規則と、暗号鍵を割り当てる、(2)各ブロックは、割り当てられた鍵で暗号化された状態で、自由に機器間を転送あるいは通常の記憶領域（通常記憶部）に保存される、(3)コンテンツ中の一部のブロックに逐次的な再生を強制する必要がある場合は、コンテンツデータとは別の独立したデータとしてその利用規則を作成し、コンテンツデータに関連付ける、(4)記憶装置内に、他の正規の機器との間で認証を完了した後アクセスが可能になる特殊な領域（保護記憶部）を通常記憶部とは別に設け、鍵やブロックに固有の利用規則等のデータを保存する。

第3章では、本研究で想定する利用規則の内容を明確化し、この利用規則に沿った利用制御を記憶装置主導で実現するために、ホスト装置と記憶装置、あるいは2つの記憶装置間で実行されるべき処理シーケンスの概要を提案している。想定される利用規則は、デジタルテレビ放送コンテンツに対して実際に設けられている複製回数に関する制約、及びコンテンツに含まれるCM部の再生の強制を想定したコンテンツの一部に対する逐次再生の強制及びそれ以外の部分に対するランダム再生の許可に関するものである。

第4章では、コンテンツデータと第2章で導入したコンテンツ復号鍵及び2種類の利用規則を具体的に関連付ける仕組みを提案している。具体的には、Windows及びLinux双方の基本ソフトウェアに実装されているファイルシステムであるUDFを基礎として、そこで規定されているNamed Streamと呼ばれるメタデータを拡張することで、この仕組みを実現した。この関連付けの仕組みには、ある一連のブロックの逐次的再生の強制と、その再生完了後に一部のブロックに対してランダムアクセスを許可するといった内容の規則の改竄を検知する仕組みも組み込まれている。

第5章では、各ブロックを適切に暗号化するために、商用デジタルコンテンツを保存する記憶媒体として広く利用されているBlu-rayディスクにおいて採用されている暗号化方式を元にして、HDD装置及びUDFファイルシステムの特性に合い、且つ攻撃に対する暗号文の強度がより高くなるような方式を提案している。さらに、この方式による暗号化だけでは、コンテンツを分割する際に、ホスト装置が分割点を含むブロックの復号と再暗号化する必要があるという問題があることを指摘し、当該処理を実行せずに済むようにするための仕組みも提案している。

第6章では、各ブロックを暗復号するための鍵や利用規則等を転送し合う2つの機器が互いを認証し合う仕組み、及び認証を完了した2つの機器間で、安全に、且つ利用規則に違反した複製が行われたり、消失したりせずに転送するための仕組みを提案している。

第7章では、実際の家電機器やHDDに搭載されているプロセッサやハードウェア暗復号エンジンがホスト装置や記憶装置に搭載されていると仮定した上で、コンテンツに対していくつかの典型的な操作（複製と通常再生，あるいは複製と早送り再生の並列実行等）を行った場合に、コンテンツの保存や再生が問題なく実行できるという評価結果を提示している。

第8章では、本研究で得られた研究成果をまとめている。

注)論文内容の要旨と論文審査の結果の要旨は１頁を３８字×３６行で作成し、合わせて、３，０００字を標準とすること。
論文内容の要旨を英語で記入する場合は、４００～１，１００wordsで作成し
審査結果の要旨は日本語５００～２，０００字程度で作成すること。

（続紙 ２ ）

（論文審査の結果の要旨）

本論文は、ハードディスク装置（HDD）を代表とするプロセッサを内蔵した記憶装置の特性を利用して、攻撃に対する高い堅牢性を備え、記憶装置に保存された商用動画コンテンツを不特定のホスト装置で利用できるようにするためのアクセス制御（利用制御）機構の体系を提案したものである。

学位申請者は、HDDに代表されるプロセッサを内蔵する記憶装置に相手機器の認証、及び、利用制御上の主要な処理を行わせるための仕組みを、本研究で考案している。この仕組みを搭載したシステムは、従来の機器に比べて、高い利便性と攻撃に対する高い堅牢性を備えることができる。

本研究において得られた成果の概要は、以下の通りである。

1. 商用動画コンテンツを対象とした利用制御を記憶装置が自律的に実現するためのアーキテクチャを提案した。その概要は、(1)動画コンテンツを適切な大きさのブロックに分割し、個々のブロックに、他のブロックの利用実績に依存しない各ブロックに固有の利用規則と、暗号鍵を割り当てる、(2)各ブロックは、割り当てられた鍵で暗号化された状態で、自由に機器間を転送あるいは通常の記憶領域（通常記憶部）に保存される、(3)コンテンツ中の一部のブロックに逐次的な再生を強制する必要がある場合は、コンテンツデータとは別の独立したデータとしてその利用規則を作成し、コンテンツデータに関連付ける、(4)記憶装置内に、通常記憶部の他に、他の正規の機器との間で認証を完了した後アクセスが可能になる特殊な領域（保護記憶部）を設け、鍵やブロックに固有の利用規則等のデータは、記憶装置内の保護記憶部に保存する、というものである。
2. 利用規則に沿った利用制御を記憶装置主導で実現するために、ホスト装置と記憶装置（コンテンツの通常・逐次再生）、あるいは、2つの記憶装置間（コンテンツの複製）で実行されるべき処理シーケンスを明らかにした。
3. コンテンツデータとコンテンツ復号鍵及び2種類の利用規則を関連付ける仕組みを、UDFのNamed Streamと呼ばれるメタデータを拡張することで実現した。一連のブロックの逐次的再生の強制と、その再生完了後に一部のブロックに対してランダムアクセスを許可するといった内容の規則の改竄を検知する仕組みも組み込むことで、規則データの完全性を担保した。
4. Blu-rayディスクの暗号化方式を参考に、ハードディスク装置及びUDFファイルシステムの特性に合い、且つ攻撃に対する暗号文の強度がより高くなることを目的とする暗号化方式を考案した。従来の方式だけでは、コンテンツを分割する際に、分割点を含むブロックの復号と再暗号化をホスト装置が行う必要があるという問題があることを指摘し、当該処理を実行せずに済むようにするための仕組みも提案した。
5. 各ブロックを暗復号するための鍵や利用規則等を、正当な2つの機器間で安全に、且つ利用規則に違反した複製が行われたり、消失したりせずに転送するための仕組みを提案した。記憶装置に固有の内部の挙動も考慮した認証、鍵及び利用規則の転送、及び復旧の仕組みを提案するとともに、コンテンツに対していくつかの典型的な操作（複製と通常再生、あるいは複製と早送り再生の並列実行等）を行った場合に、コンテンツの保存や再生が問題なく実行できることを示した。

以上のとおり、本論文では、ホスト装置に対する着脱性を備えたHDDに代表される大容量の記憶装置が、主体的・自律的に利用制御を行う上で、新規性・有用性の高い仕組みを提案している。デジタルテレビ放送において配信されるコンテンツの容

量が増大し、インターネットを介して膨大な量の入手可能な音楽や動画コンテンツの入手が可能になった現在、本研究で提案した数々の仕組みは、今後商用デジタルコンテンツの流通形態や利用規則が多様化した場合においても、十分貢献できるものと認められる。

このように、本研究成果は学術上寄与するところが少なくないため、博士（情報学）の学位論文として価値あるものと認める。また、平成28年6月10日に、論文内容とそれに関連した事項について学力試問を行った結果、合格と認めた。